Security and Compliance at Rievent (2020)

Rievent meets the compliance and security requirements of medical organizations, publishers, continuing education providers, universities, government customers, and hospitals.

Accessibility

Rievent committed to meeting accessibility requirements.

The Rievent VPAT™ Accessibility Conformance Report (WCAG edition) is available upon request. Rievent strives to meet or exceed W3C Web Content Accessibility Guidelines (WCAG) 2.1 Level A and Level AA success criteria.

A Voluntary Product Accessibility Template (VPAT™) explains how information and communication technology (ICT) products relate to the Revised 508 Standards for IT accessibility.

Privacy

We've developed a Privacy Policy that covers how Rievent products and services collect, use, disclose, transfer, and store end user and customer information. The policy is available at the bottom of Rievent product web pages.

Rievent's products and services are frequently embedded within our customers' websites, or Rievent hosts sites for our customers with their branding and website wrappers. Our customers share the responsibility to maintain and respect the privacy of end users.

Rievent conforms to United States and international privacy consumer and Internet privacy laws, a shared responsibility with our customers. Rievent follows US federal and State data breach notification law (in coordination with customers), disposal of records laws, personal information handling and security requirement laws, social security number restrictions (Rievent will not store or collect SSNs), identity theft protection laws, and data security measures as required by law.

Rievent conforms to the following privacy standards and laws:

International

- European Union General Data Protection Regulation (GDPR). Rievent and Rievent's customers share privacy compliance responsibility; Under GDPR, Rievent is a Data Processor, customers are Data Controllers.

Federal

- United States Federal Trade Commission's Fair Information Practices (US FTC FIP)
- Federal CAN-SPAM act

State

- California Consumer Privacy Act of 2018 (CCPA)
- California Online Privacy Protection Act of 2014 (CalOPPA)
- Rievent complies with additional states' laws, with CCPA and GDPR providing comprehensive guidelines exceeding or including requirements of other states in most cases.

Information Security

Rievent follows industry best practices for information security.

Rievent uses the U.S. Department of Commerce National Institute of Standards and Technology (NIST) Cybersecurity Framework to guide its security practices. The Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. The Framework is the go-to resource for Rievent when evaluating and developing security practices and software standards.

NIST SP-800-53 Rev. 4 & 5 is Rievent's primary security and privacy control specification and overrules any conflicting or older standards.

Rievent has completed the Payment Card Industry (PCI), Data Security Standard (DSS), Self-Assessment Questionnaire A and Attestation of Compliance. Rievent is a card-not-present (ecommerce) provider, all card processing is fully outsourced with no electronic storage, processing, or transmission of cardholder data on within Rievent software or systems. Rievent is integrated with PayPal and Authorize.Net as e-commerce processors.

Rievent is hosted at Amazon Web Services. Service Organization Controls (SOC) reports (SSAE 18 and ISAE 3402 standards), ISO, and additional reports are available from Amazon.

HIPAA and HITRUST CSF are not required for continuing education.

Customers may request Rievent review or meet additional standards at their expense.

Business Continuity and Disaster Response Planning

Rievent uses fault tolerance techniques including real-time data replication, geographically pre-staged remote recovery locations, and daily backups. Rievent maintains and tests internal business continuity disaster preparedness and recovery plans. Rievent uses 24/7 electronic uptime and security monitoring of its services and web sites, and system engineers are on call to receive alerts and respond to outages and incidents. Rievent maintains redundant systems with a capability to recover systems in a geographically remote pre-staged location. Rievent databases are hosted on Amazon Web Services utilizing multi-availability zone mirroring, daily backups archived to a geographically distant emergency recovery region, and an additional full read-replica is also maintained in real time.

Rievent’s customer contract provides a Service Level Agreement (SLA) with a 99.9% uptime guarantee.

Identity and Access Management (IAM) and Single Sign-On

Single sign-on between customer systems and Rievent is available using the Rievent secure Trusted Handoff Protocol. Developers register security credentials (public key) with the Rievent Platform then package and digitally sign security credentials along with user information to securely authenticate and synchronize users with Rievent sites by passing a digitally signed and optionally encrypted JSON Web Token (JWT) (over HTTPS). Customers may also bridge or proxy from Security Assertion Markup Language (SAML) or OpenID Connect (OIDC) Identity and Access Management systems to provide seamless single sign-on. Contact Rievent for more information.